KXChang

KXChang

Key Exchange Algorithm

KXChang

- Invented in 2019
- Reference implementation in Python

Design Goals

- To be resistant to DLP attacks
- To have smaller key lengths than traditional DiffieHellman

Key Generation

- Generate 2 N bit integers, let A be the public modulus and let B be the public key
- Choose a integer in B between 1 and N – 1 and let that be the secret key

Key Exchange Setup

- Alice and Bob generate SK, PK, N
- Either Bob or Alice sends their public key over
- Alice and Bob both send their public keys over

Key Exchange Phase 1

- Alice and Bob have chosen to use Bob's public key. Alice and Bob both raise Bob's public key to their secret exponent modulo the shared modulus. They exchange phase 1.

Key Exchange Phase 2

- Alice and Bob compute phase1 raised to their secret exponent modulo N arriving at the secret modulus.

Key Exchange Phase 3

- Alice and Bob raise Alice's public key to the power of their secret key modulo the secret modulus. They transmit phase3 to each other.

Key Exchange Phase 4

- Alice and Bob raise phase3 to their secret exponent modulo the secret modulus arriving at the shared secret.

Cryptanalysis

- TBD